



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Ascom IP-DECT Solution with Avaya IP Office 11.0 - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless interoperability between Ascom Wireless IP-DECT with Avaya IP Office release 11.0.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Ascom's IP-DECT solution to interoperate with Avaya IP Office. Ascom's IP-DECT handsets are configured on the IP Avaya Office as SIP users, therefore enabling them to make/receive internal and PSTN/external calls and have full voicemail and other telephony facilities available on Avaya IP Office. The Wireless communication is made using Ascom IP-DECT Access points connected to the same LAN as the Avaya IP Office.

The Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as the secondary expansion cabinet. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and user names. This allows calls between systems and support for a range of internal call features.

The Ascom IP-DECT system is a modular solution for large and small deployments with full handover capabilities within one PBX. The Ascom IP-DECT Access points works as a conduit between the Avaya IP Office and the Ascom IP-DECT wireless handsets. After the Ascom IP-DECT wireless handsets register with the Ascom IP-DECT Access points, the Access points registers the handsets to Avaya IP Office.

- IP (Internet Protocol) – Universal standard for inter-networking that maximizes scalability and interoperability.
- DECT (Digital Enhanced Cordless Telecommunications) - Secure radio communication standard that delivers superior voice quality over reserved radio frequency bands.

2. General Test Approach and Test Results

The general test approach was to configure the Ascom IP-DECT handsets to communicate with IP Office as implemented on a customer's premises. The interoperability compliance testing evaluates the ability of the Ascom IP-DECT handsets (DECT handsets) to make and receive calls to and from Avaya H.323, SIP, Digital desk phones and PSTN endpoints. The integrated IP Office Voicemail was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication and DTMF on the DECT handsets. See **Figure 1** for the network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

Note: For compliance testing the Ascom DECT handsets were registered to the primary server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and DECT handsets did not include use of any specific encryption features as requested by Ascom.

Note: Compliance testing was carried out using TCP as the transport for signaling, a selection of basic calls and transfer calls were carried out using UDP.

2.1. Interoperability Compliance Testing

Tests were performed to ensure full interoperability between the DECT handsets and IP Office. The tests were all functional in nature and performance testing was not included. The testing included:

- Registration/Invalid Registration
- Basic Calls, local and PSTN
- Hold and Retrieve
- Attended and Unattended Transfer
- Call Forwarding Unconditional, No Reply and Busy (Local and PBX)
- Call Waiting
- Call Park/Pickup
- Do Not Disturb

- Calling Line Name/Identification
- Codec Support
- DTMF Support
- Message Waiting Indication
- Mobile Twinning
- Hunt Groups
- Serviceability Testing

2.2. Test Results

All test cases were carried out with positive results. There were some observations and some issues noted as follows.

- Expires timer on IP Office is hard coded at 180 seconds. Recommend this be used on handsets for Expires timer.
- It is recommended that “Call Waiting” on IP Office and IP-DECT is turned off. There is a scenario with DECT and semi-attended transfers where the “transfer target” and “initial caller” DECT handsets hang up whilst a second party is ringing to the “transferor” during transfer. If a call is made to the “transferor” DECT handset with Call Waiting enabled the handset accepts the call but the ringing call is cancelled. This behaviour is seen using a single R<extn> method to transfer calls. When Call waiting is off, on the IP Office (and IP-DECT base station), the call to the transferring handset shows busy until the transferred call is answered. When the RR<extn> method is used for transferring, a call can be placed to the transferring handset as this method completes the transfer on hang up. This is as per design.
- Codec G722.2 (AMR-WB) is not supported on IP Office but is on the IP-DECT.
- It is recommended that IP Office is used for call diversion.
- Registering with Invalid Credentials on IP Office causes the device to be “blacklisted”. Avaya are investigating the issue. A restart of the IP Office resolves the problem as a workaround. There is no issue with registration with correct credentials.
- When Digital set makes a transfer between two DECT sets there is no RTP after the Blind transfer is complete. No issue on Supervised Transfer for the same scenario. Avaya are investigating the issue.

2.3. Support

Technical support from Ascom can be obtained through the following:

Phone: +46 31 559450

E-mail: support@ascom.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an IP Office which the DECT handsets were configured as SIP users. The Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as the secondary expansion server. Digital, H.323 and SIP phones were configured on the IP Office. QSIG and SIP trunks were configured to simulate connections to the PSTN. The Ascom Master Access point was connected to the IP Network which the IP-DECT handsets register to. The Roaming Access point allows radio communication between the IP-DECT handsets which in turn communicates with IP Office.

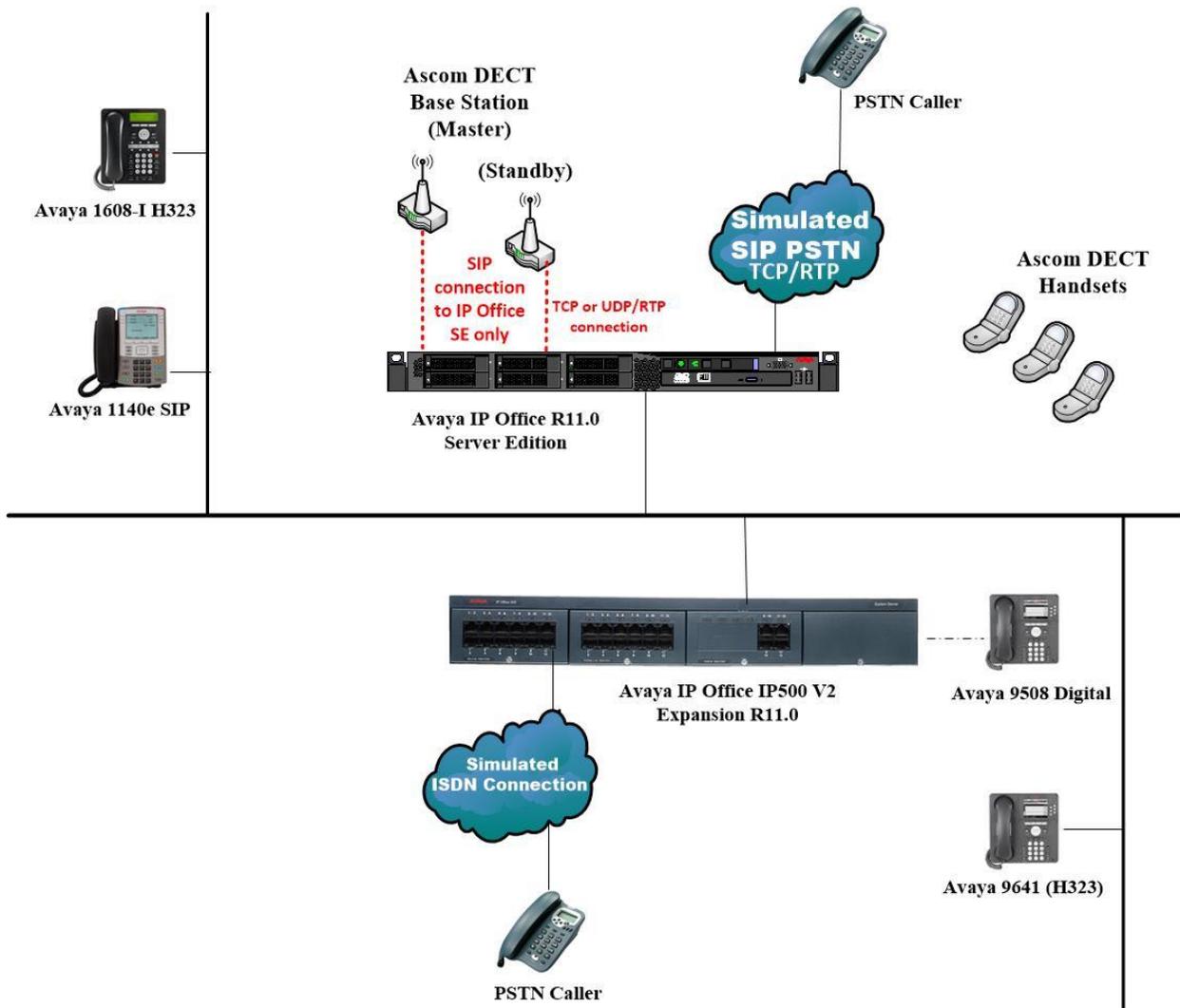


Figure 1: Avaya IP Office and Ascom Reference Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya IP Office Server Edition running on a Virtual Platform	11.0.0.1.0 Build 8
Avaya IP Office IP500 V2	11.0.0.1.0 Build 8
Avaya IP Office Manager running on a Windows 7 PC	11.0.0.1.0 Build 8
Avaya 1608-I H323 Deskphone	1608UA1_350B.bin
Avaya 9641 H323 Deskphone	R6.6115
Avaya 1140e SIP Deskphone	R04.04.28.00
Avaya 9508 Digital Deskphone	V0.6
Ascom IP DECT handsets (d81) Ascom IP DECT handsets (d63)	4.6.2 2.2.2
Ascom IP Base Station (IPBS2)	10.2.9 [Bootcode 10.2.9]

5. Avaya IP Office Configuration

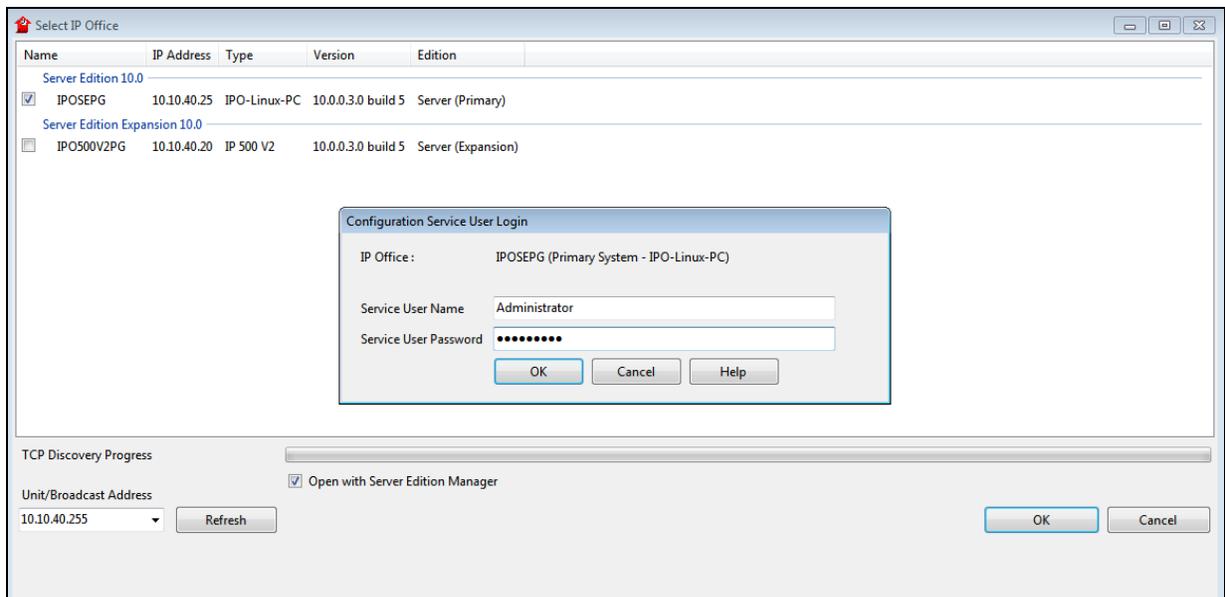
Configuration and verification operations on Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of Avaya IP Office for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Launch Avaya IP Office Manager (Administration)
- Display LAN Properties
- Create a new User
- Check Extension Properties
- Verify the Voicemail Collect Short Code
- Save Configuration

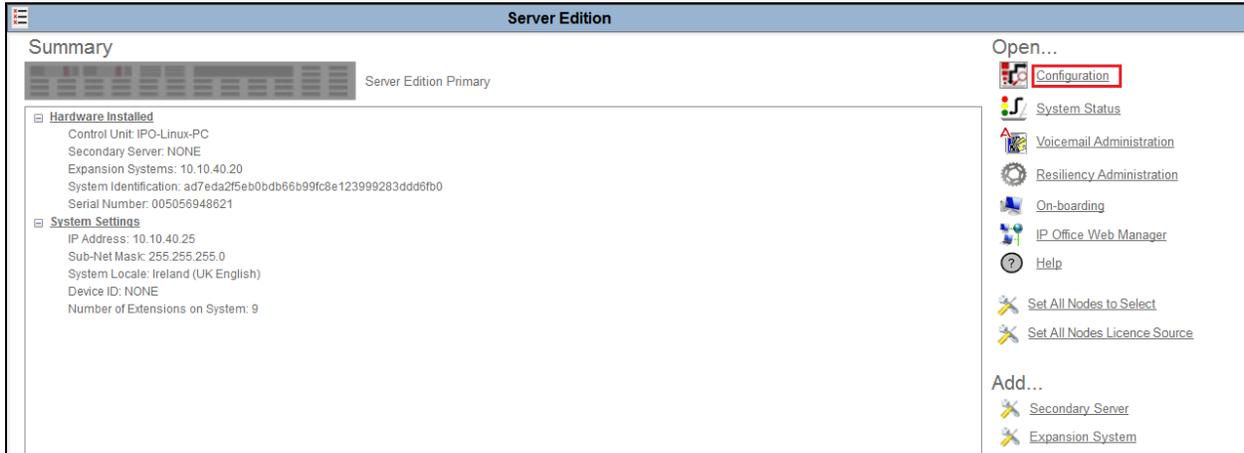
Note: Only the unique prompts are shown in the screen captures below, all other inputs can be left at default.

5.1. Launch Avaya IP Office Manager (Administration)

From the IP Office Manager PC, click **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application (not shown). Select the required Server Edition as shown below and enter the appropriate credentials. Click on the **OK** button.

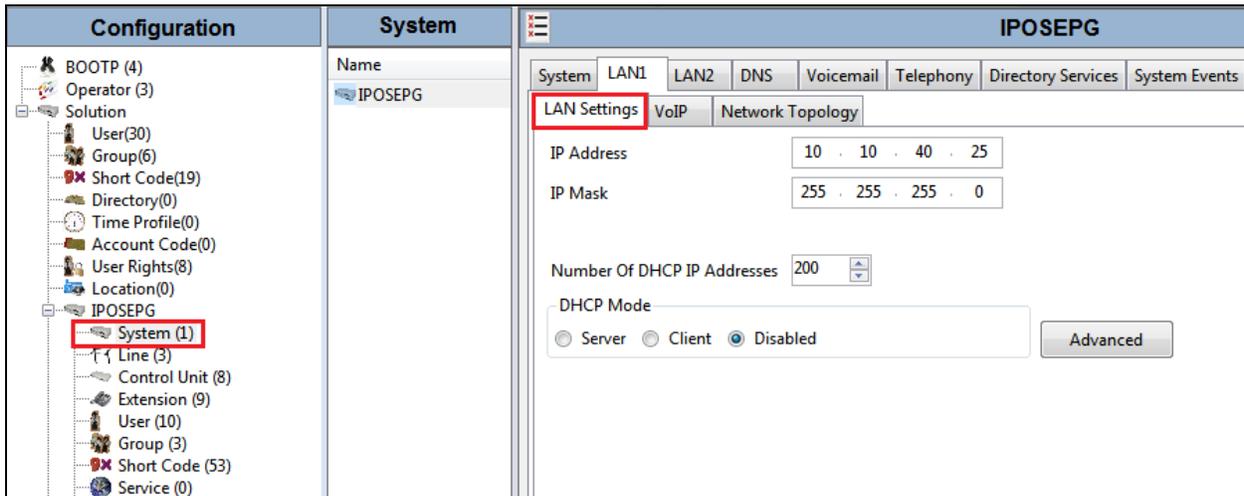


Click on **Configuration** at the top right of the page, as shown, to receive the IP Office configuration.

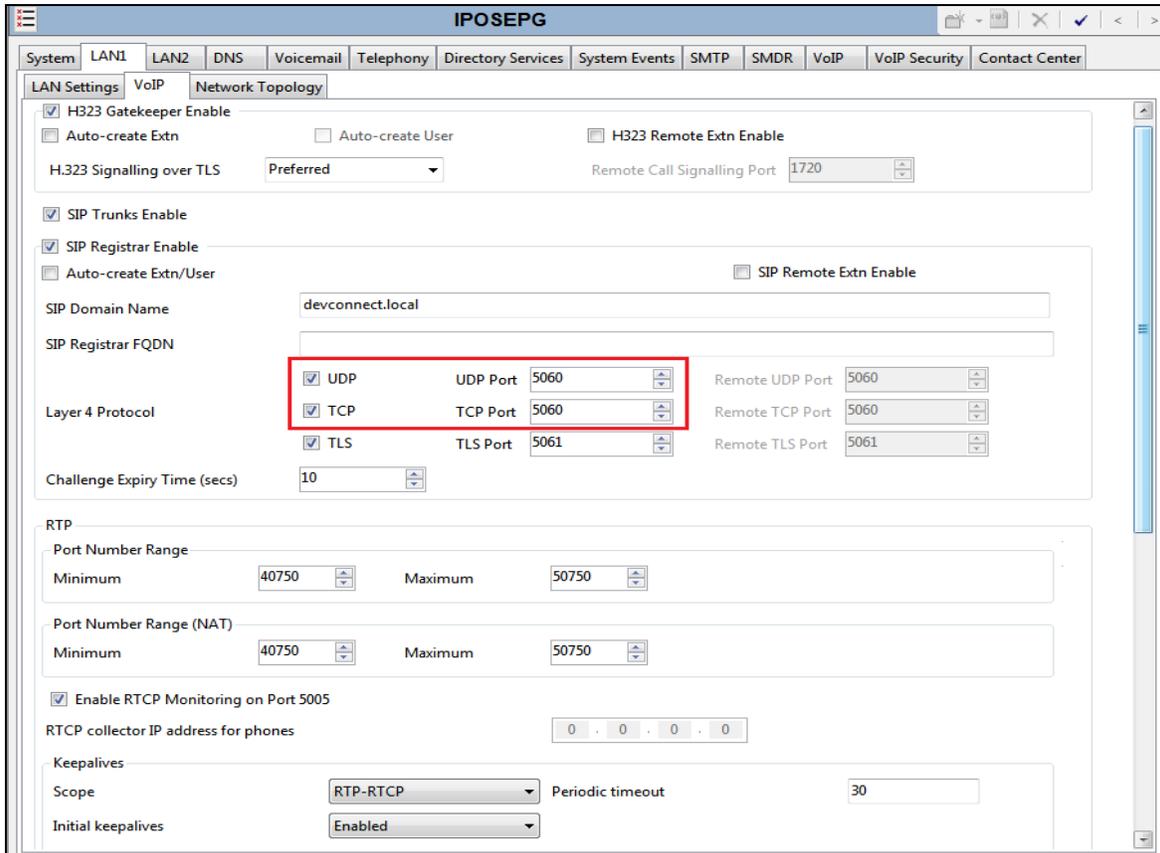


5.2. Display LAN Properties

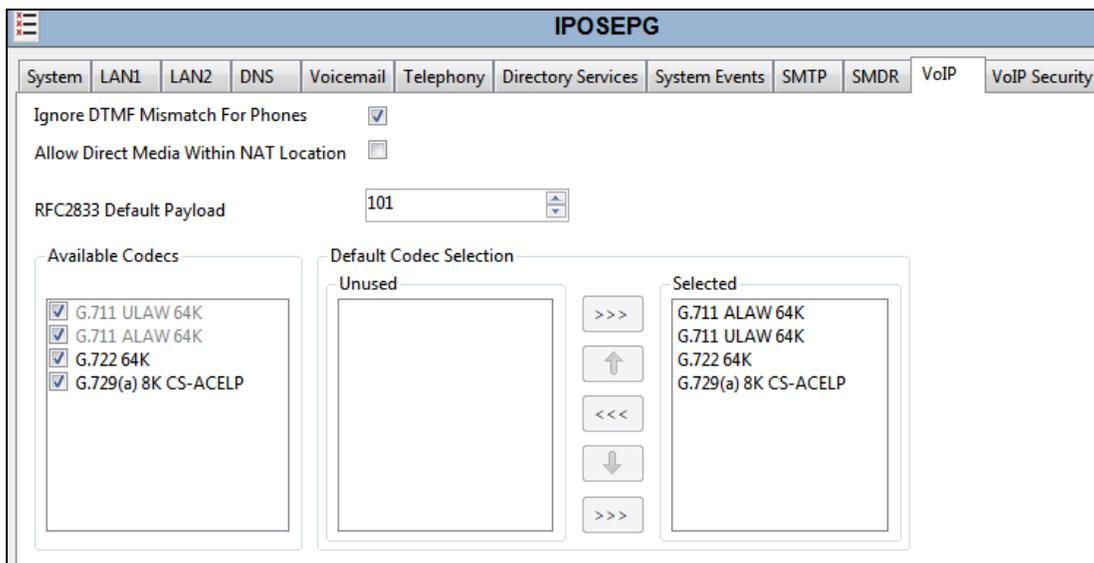
From the left window navigate to **System (1)** as shown and in the main window click on the **LAN1** tab and within that tab select the **LAN Settings** tab. The **IP Address** of the IP Office is shown, and this will be required for setup in **Section 6.1**.



Within the **LAN1** tab, click on the **VoIP** tab. Ensure that **TCP** and **UDP** boxes are checked and that port **5060** is being used. During compliance testing **RTP-RTCP Keepalives** were set to **30** secs.

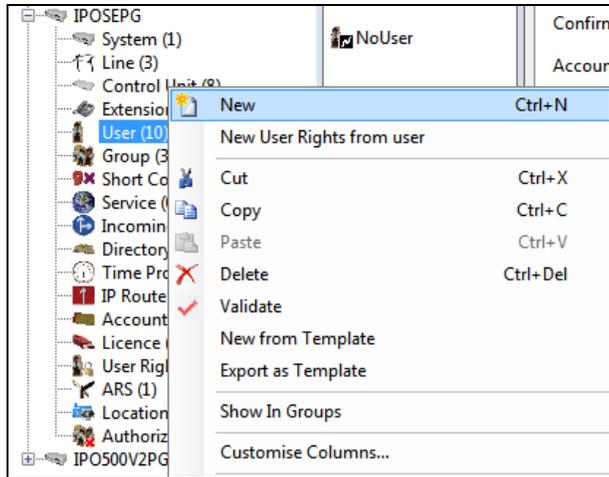


The Codec and DTMF settings can be changed under the **VoIP** tab as shown below.



5.3. Create a new User

From the left window, right click on **User** and select **New**.



In the **User** tab add a **Name** and **Password** along with the **Extension**.

A screenshot of a web application interface for configuring a user. The title bar shows '5180: 5180'. The 'User' tab is active, with other tabs like Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, and Mobility. The form fields are: Name (5180), Password (masked with dots), Confirm Password (masked with dots), Unique Identity (empty), Audio Conference PIN (empty), Confirm Audio Conference PIN (empty), Account Status (Enabled), Full Name (MYCO SE 5180), Extension (5180), Email Address (empty), Locale (dropdown), Priority (5), System Phone Rights (None), Profile (Basic User), and a list of checkboxes for user roles: Receptionist, Enable Softphone, Enable one-X Portal Services, Enable one-X TeleCommuter, Enable Remote Worker, Enable Communicator, Enable Mobile VoIP Client, Send Mobility Email, and Web Collaboration.

Under the **Voicemail** tab, **Voicemail On** can be selected to provide voicemail to this user/extension.

5180: 5180

User | **Voicemail** | DND | ShortCodes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming

Voicemail Code: ●●●●

Confirm Voicemail Code: ●●●●

Voicemail Email: [Empty Field]

Voicemail On

Voicemail Help

Voicemail Ringback

Voicemail Email Reading

UMS Web Services

Enable GMAIL API

Voicemail Email: Off Copy Forward Alert

DTMF Breakout

Reception / Breakout (DTMF 0): System Default ()

Breakout (DTMF 2): System Default ()

Breakout (DTMF 3): System Default ()

Under the **Telephony** tab and **Call Settings** tab, **Call Waiting On** can be turned on/off depending on what is required by the user.

5180: 5180*

User | Voicemail | DND | ShortCodes | Source Numbers | **Telephony** | Forwarding | Dial In | Voice Recording | Button Programming

Call Settings | Supervisor Settings | Multi-line Options | Call Log | TUI

Outside Call Sequence: Default Ring

Inside Call Sequence: Default Ring

Ringback Sequence: Default Ring

No Answer Time (secs): System Default (15)

Wrap-up Time (secs): 2

Transfer Return Time (secs): Off

Call Cost Mark-Up: 100

Advertise Callee State To Internal Callers: System Default (Off)

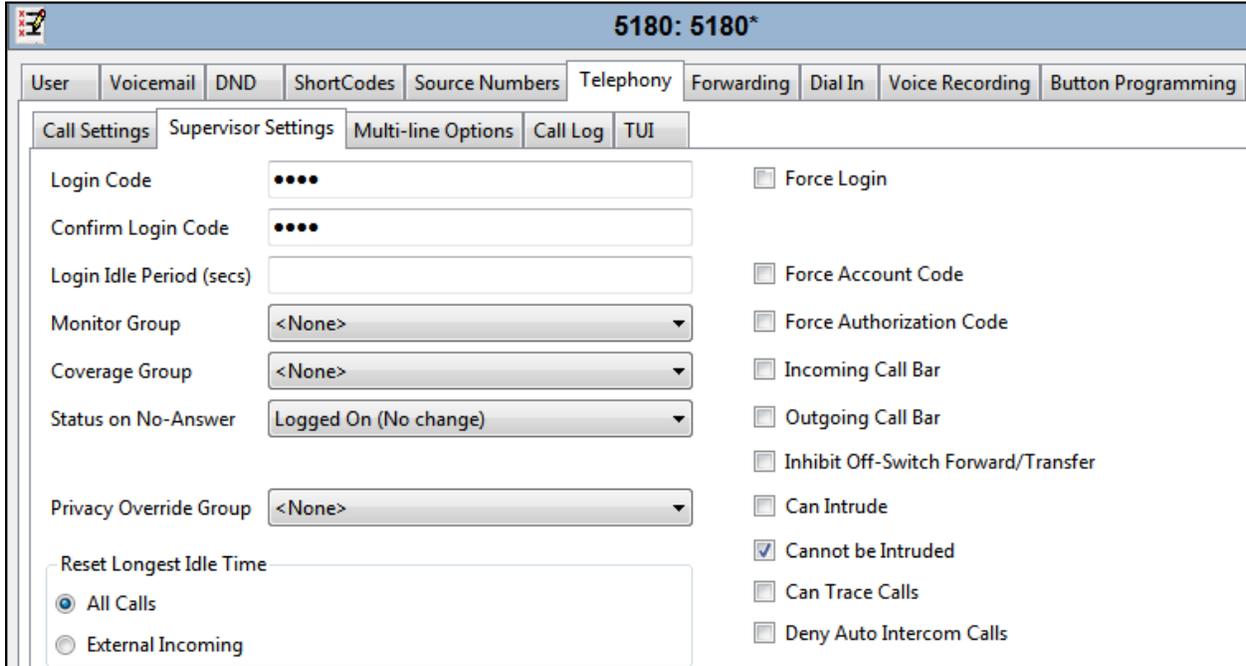
Call Waiting On

Answer Call Waiting On Hold

Busy On Held

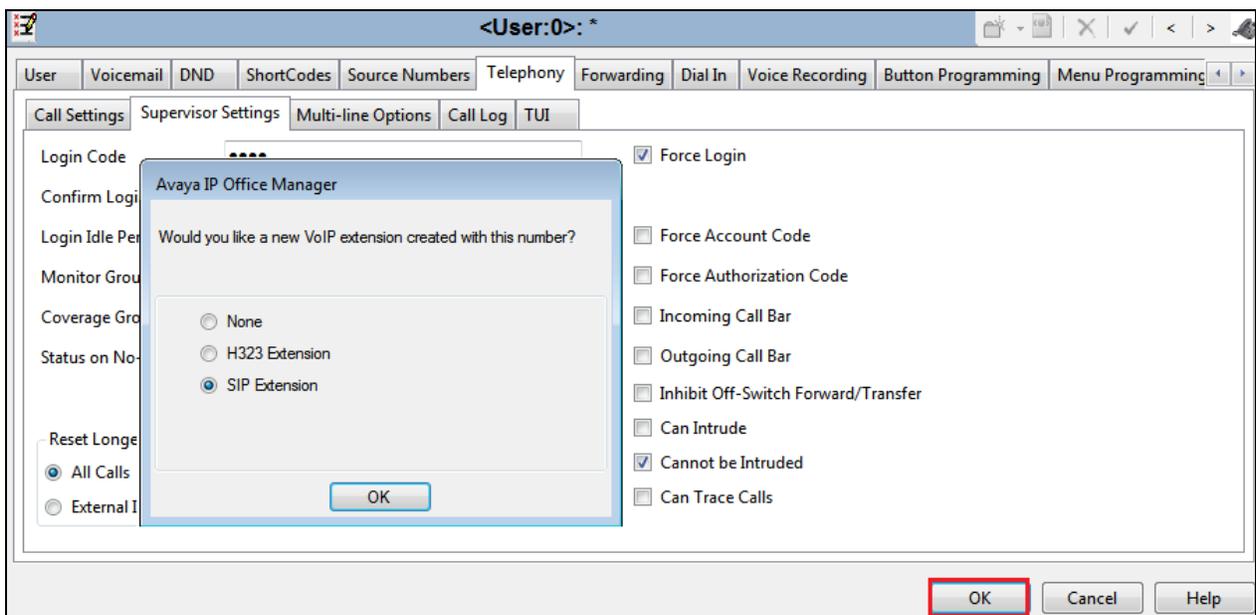
Offhook Station

Under **Supervisor Settings** tab enter the password again for the **Login Code**.



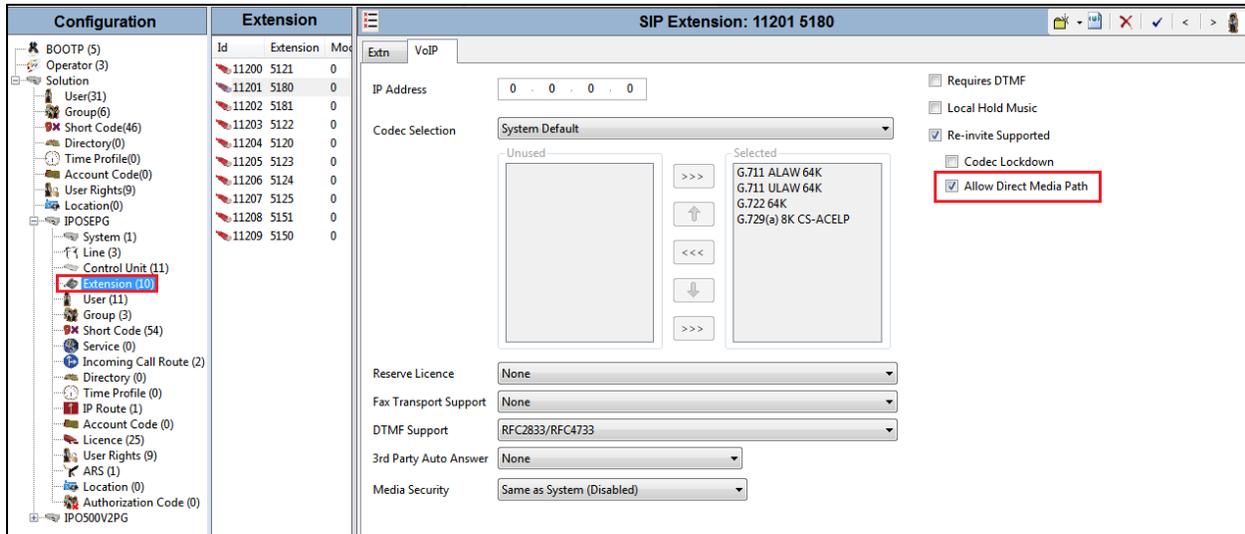
Once **OK** is clicked at the bottom of the screen a new window should appear asking to create a new extension. Select **SIP Extension** as is shown below.

Note: If the system is not setup to auto-create extensions, then a new extension can be added by right-clicking on Extension on the left window and selecting **New**, (not shown).



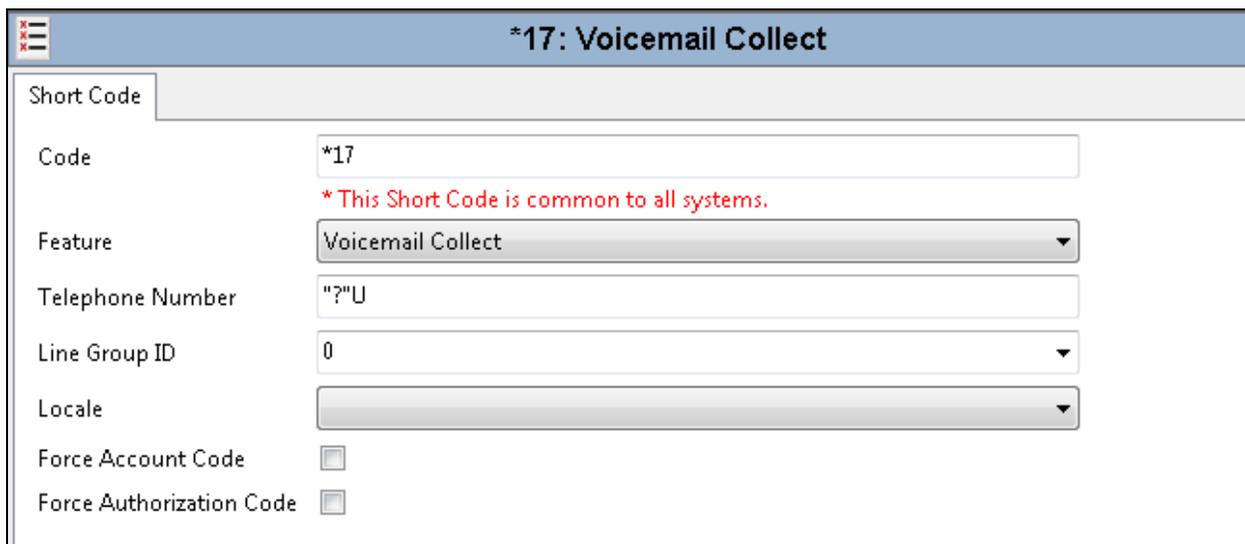
5.4. Check Extension Properties

Direct Media Path can be set on/off in the extension properties. This will allow RTP to be sent directly between devices. Once the SIP extension has been successfully created in **Section 5.3**, open the extension configuration to check to see if Allow Direct Signalling is selected. Select **Extension** in the left window and select the required extension number. In the main window under **VoIP** tab, **Allow Direct Media Path** can be checked or unchecked as shown below. Other settings such as **DTMF Support** and **Codec Selection** are possible to change here as well again if required by Ascom.



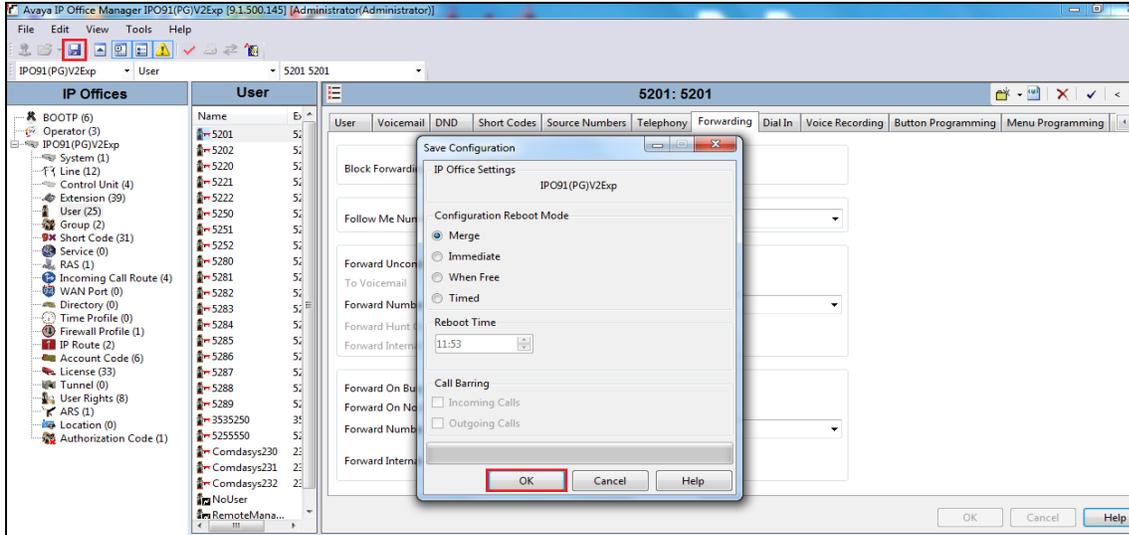
5.5. Verify the Voicemail Collect Short Code

As part of the Ascom IP-DECT Base Station configuration the Voicemail access number is required. During compliance testing this **Feature** was set to **Voicemail Collect**, and the **Code** was ***17** also the **Telephone Number** was **"?"U**.



5.6. Save Configuration

Once all the configurations have been made it must be saved to IP Office. Click on the **Save** icon at the top of the screen and the following window appears. Click on **OK** to commit the changes to memory.



6. Configure Ascom IP-DECT

This section describes how to access and configure the Ascom DECT solution. The Ascom wireless IP-DECT Base Stations can be configured in a Master/Standby Master scenario to provide redundancy or to extend the radius of coverage (roaming). The following configuration steps detail the configuration process used to configure an Ascom wireless IP-DECT Base Station in Master mode only.

Roaming between multiple Ascom Wireless IP-DECT Base Stations as shown in **Figure 1** was tested but the configuration setup will not be shown in this document. Refer to the Ascom document in **Section 9** for information on how to configure roaming.

6.1. Configure the IP-DECT Base Station

To configure the IP-DECT Base Station, access a web browser and enter the IP address of the Base Station as the URL. The user will be presented with the screen shown below. Click the **System administration** link and enter the appropriate credentials to access the Ascom wireless IP-DECT Base Station and then click **OK** (not shown).



6.1.1. General Configuration of IP-DECT Base Station

When the new window opens navigate to **General** and select the **Admin** tab and enter the following:

- **Device Name** Enter a descriptive name that identifies this Ascom wireless IP-DECT Base Station
- **User Name** Enter the **User Name** (the default User name was used)
- **Password** Enter the **Password** (the default Password was used)
- **Confirm Password** Confirm the password

Click the **OK** button to continue.

The screenshot shows the 'IP-DECT Base Station' configuration window with the 'Admin' tab selected. The 'Local Admin' section is active, showing fields for 'Device Name' (INTOP R10 M), 'User Name' (admin), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). There is also a 'Login Banner' text area. Below this, the 'Local Security Policy' section includes 'Automatic Logout after' (with a [min] dropdown), 'Limit Sessions to' (with dropdowns for 'per system' and 'per user'), and checkboxes for 'Disable Native Authentication' and 'Require Certificate'. The 'Delegated Authentication' section has a 'Join realm' link. The 'Additional Kerberos encryption types' section has an 'Enable AES and RC4' checkbox. The 'Authentication Servers' table has columns for 'Realm/Domain', 'IP Address', 'Port', 'Admin Port', 'Secondary IP Address', 'Secondary Port', 'Secondary Admin Port', and 'Delete'. At the bottom are 'OK' and 'Cancel' buttons.

6.1.2. Configure LAN DHCP

Navigate to **LAN** and select the **DHCP** tab. Select **Disabled** from the **Mode** dropdown box. A reset of the base station is required to activate this setting. After the reset is completed log back on to the IP-DECT Base Station to complete the configuration.

The screenshot shows the 'IP-DECT Base Station' configuration window with the 'LAN' tab selected. The 'DHCP4' sub-tab is active, showing a 'Mode' dropdown menu set to 'disabled' with the text 'Currently - disabled' next to it. Below the dropdown are 'OK' and 'Cancel' buttons. The left sidebar shows the navigation menu with 'LAN' selected under the 'Administration' section.

6.1.3. Configure LAN IP

Navigate to **LAN** and select the **IP** tab and enter the following:

- **IP Address** Enter the IP address to be assigned to the IP-DECT Station
- **Network Mask** Enter the Network Mask to be assigned to the IP-DECT Station
- **Default Gateway** Enter the Default Gateway IP Address

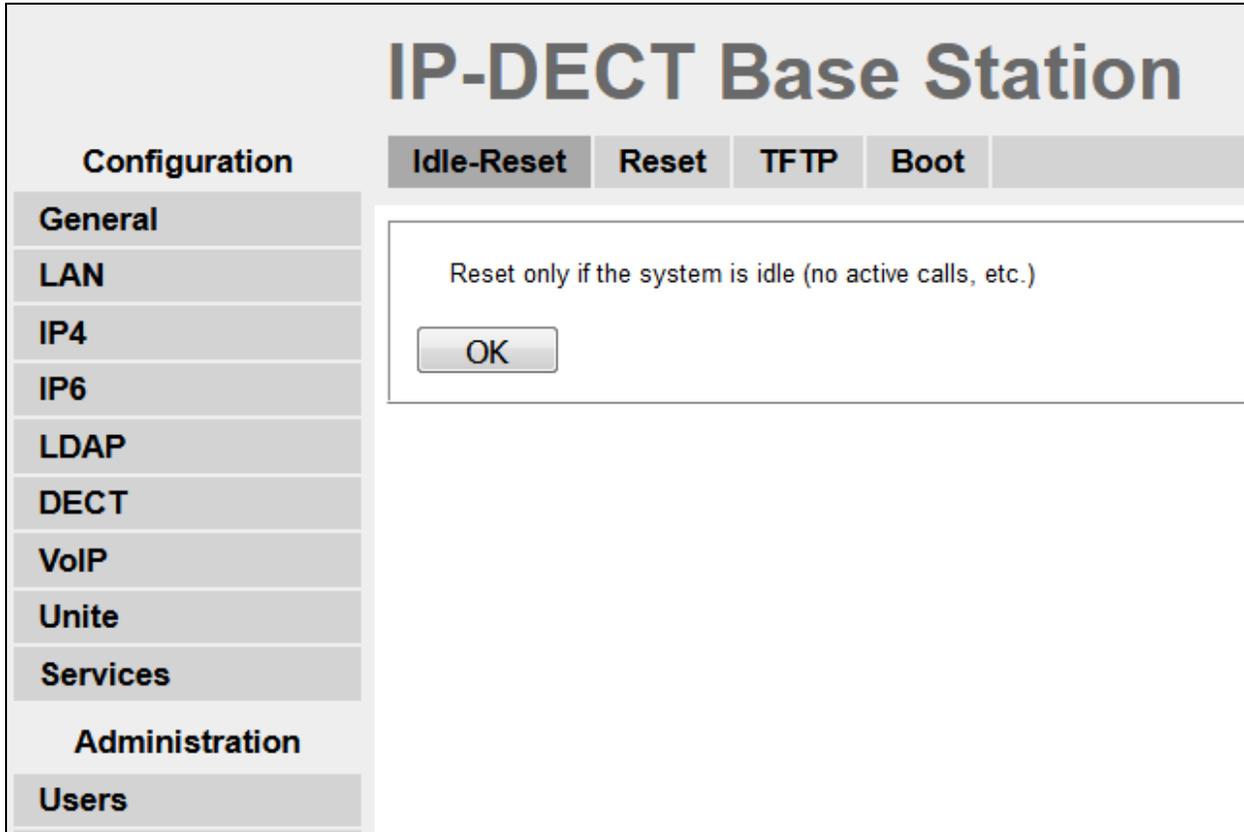
Click on the **OK** Button to save.

Note: No DNS entries were made for compliance testing.

The screenshot displays the configuration interface for an IP-DECT Base Station. The main title is "IP-DECT Base Station". Below the title is a navigation bar with tabs for "DHCP4", "IP4", "DHCP6", "IP6", "VLAN", "Link", "802.1X", "Statistics", and "LLDP". The "IP4" tab is selected. On the left side, there is a vertical menu with options: "Configuration", "General", "LAN", "IP4", "IP6", "LDAP", "DECT", "VoIP", "Unite", "Services", "Administration", "Users", "Device Overview", "DECT Sync", and "Traffic". The "LAN" and "IP4" options are highlighted. The main content area shows the "Active Settings" for the IP4 configuration. It includes fields for "IP Address" (10.10.40.126), "Network Mask" (255.255.255.0), "Default Gateway" (10.10.40.1), "DNS Server" (10.10.40.1), and "Alt. DNS Server" (empty). There is also a "Check ARP" checkbox which is unchecked. Below these settings is a section for "Static IP Routes" with a table header: "Network Destination", "Network Mask", and "Gateway". The table has three empty input fields. At the bottom of the configuration area are "OK" and "Cancel" buttons.

6.1.4. Reset IP-DECT Base Station

Click **Reset** followed by the **OK** button to initiate the system reset. Many of the other changes made to the system during the configuration process require a reset. Repeat this process whenever a reset is required.



The screenshot displays the configuration interface for an IP-DECT Base Station. The main title is "IP-DECT Base Station". On the left, there is a "Configuration" menu with the following items: General, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services, Administration, and Users. The "Reset" tab is selected in the top navigation bar, which also includes "Idle-Reset", "TFTP", and "Boot". A dialog box is open, containing the text "Reset only if the system is idle (no active calls, etc.)" and an "OK" button.

6.1.5. Configure DECT

Navigate to the **DECT** and click on the **Master** and enter the following:

- **Mode** Select **Mirror** from the dropdown box
- **Mirror Master IP address** Enter the IP Address of the Mirrored base station
- Check the **Enable PARI Function** check box
- **Protocol** Select **SIP/TCP** from the dropdown box
- **Proxy** Enter the IP address of the IP Office
- Check the **Enbloc Dialing** check box
- Check the **Allow DTMF through RTP** check box

Click the **OK** button to continue (not shown).

IP-DECT Base Station

Configuration	System	Suppl. Serv.	Master	Crypto Master	Mobility Master	Radio
---------------	--------	--------------	--------	---------------	-----------------	-------

General

Mode Mirror

Mirror Master

Mirror Status Active
Connected to 10.10.40.125

Multi-Master

Master ID

Enable PARI Function

Region Code

IP-PBX

Protocol SIP/TCP

Proxy

Alt. Proxy

Alt. Proxy

Alt. Proxy

Domain

Max. Internal Number Length

International CPN Prefix

Registration with system password

Enbloc Dialing

Enable Enbloc Send-Key

Send Inband DTMF

Allow DTMF Through RTP

Short Disconnect Tone

Treat rejected calls as Busy

Configured With Local GK

Scroll down and set **Registration Time-To-Live** to **180 (sec)**.

IPo	Configured With Local GK <input type="checkbox"/>
LDAP	SIP Interoperability Settings
DECT	Registration Time-To-Live <input type="text" value="180"/> [sec]
VoIP	STUN server <input type="text"/>
Unite	Hold Signalling <input type="text" value="inactive"/>
Services	Hold Before Transfer <input type="checkbox"/>
Administration	Accept Inbound Calls Not Routed Via Home Proxy <input type="checkbox"/>
Users	Register With Number <input checked="" type="checkbox"/>
Device Overview	AOR as Line Identity <input type="checkbox"/>
DECT Sync	KPML support <input type="checkbox"/>
Traffic	

6.1.5.1 Configure DECT System

Click on the **System** tab and enter the following:

- **System Name** Enter the System Name as previously configured
- **Password** Enter the Password as previously configured
- **Confirm Password** Confirm the Password
- **Subscriptions** Select **With System AC** from the dropdown box
- **Authentication Code** Enter the DECT handset Login code as configured in **Section 5.3**.
- **Tones** Select the location where the IP-DECT system is located
- **Default Language** Select the required Language from the dropdown box
- **Frequency** Select the required Frequency from the dropdown box
- **Enabled** Select the number of Carriers required
- Check **Local R-Key Handling** box
- Check **Disable ICE** box
- **Coder** Select the required Coder from the **Coder** dropdown box

Click the **OK** button to continue.

IP-DECT Base Station

Configuration	System	Suppl. Serv.	Master	Crypto Master	Mobility Master	Radio	Radio config
General							
LAN							
IP4							
IP6							
LDAP							
DECT							
VoIP							
Unite							
Services							
Administration							
Users							
Device Overview							
DECT Sync							
Traffic							
Gateway							
Backup							
Update							
Diagnostics							
Reset							
	System Name	<input type="text" value="DECT3"/>					
	Password	<input type="password" value="••••••••"/>					
	Confirm Password	<input type="password" value="••••••••"/>					
	Subscriptions	With System AC ▾					
	Authentication Code	<input type="text" value="9999"/>					
	Tones	EUROPE-PBX ▾					
	Default Language	English ▾					
	Frequency	1880-1900 MHz (Europe) ▾					
	Enabled Carriers	9 8 7 6 5 4 3 2 1 0 <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>					
	Local R-Key Handling	<input checked="" type="checkbox"/>					
	No Transfer on Hangup	<input type="checkbox"/>					
	No On-Hold Display	<input type="checkbox"/>					
	Display Original Called	<input type="checkbox"/>					
	Early Encryption	<input type="checkbox"/>					
	RFP Location	<input type="checkbox"/>					
	Unite Data Channel	<input type="checkbox"/>					
	Disable ICE	<input checked="" type="checkbox"/>					
	Coder	G711A ▾		Frame (ms) <input type="text" value="20"/>		Exclusive <input type="checkbox"/> SC <input type="checkbox"/>	
	Secure RTP Key Exchange	No encryption ▾					
	<input type="button" value="OK"/>		<input type="button" value="Cancel"/>				

6.1.5.2 Configure Suppl.Serv

Click on the **Suppl.Serv** tab and check the **Enable Supplementary Services** check box. During compliance testing, the IP Office handled most of the features listed, so the following functions were disabled:

- **Call Forwarding Unconditional, Call Forwarding Busy, Call Forwarding No Reply, Do not Disturb, Call waiting, Call Completion, Call Park, Interception, Call Service URI, Call Service URI (Argument), Soft Key, Logout User and Clear Local Settings**
- **MWI Mode** Select **User dependent interrogate number** from the dropdown box
- **MWI Notify Number** Enter ***17** as configured in **Section 5.5**

Click the **OK** button to continue.

IP-DECT Base Station

Configuration
System
Suppl. Serv.
Master
Crypto Master
Mobility Master
Radio
Radio config

- General
- LAN
- IP4
- IP6
- LDAP
- DECT**
- VoIP
- Unite
- Services
- Administration
- Users
- Device Overview
- DECT Sync
- Traffic
- Gateway
- Backup
- Update
- Diagnostics
- Reset

Enable Supplementary Services

	Activate	Deactivate	Disable
Call Forwarding Unconditional	.	.	<input checked="" type="checkbox"/>
Call Forwarding Busy	.	.	<input checked="" type="checkbox"/>
Call Forwarding No Reply	.	.	<input checked="" type="checkbox"/>
Do Not Disturb	.	.	<input checked="" type="checkbox"/>
Call Waiting	.	.	<input checked="" type="checkbox"/>
Call Completion	.	.	<input checked="" type="checkbox"/>
Call Park	.	.	<input checked="" type="checkbox"/>
Interception	.	.	<input checked="" type="checkbox"/>
Call Service URI	.		<input checked="" type="checkbox"/>
Call Service URI (Argument)	.		<input checked="" type="checkbox"/>
Soft key	.		<input checked="" type="checkbox"/>
Logout User	.		<input checked="" type="checkbox"/>
Clear Local Setting	.		<input checked="" type="checkbox"/>
MWI Mode	User dependent interrogate number ▼		
MWI Notify Number	*17		
Local Clear of MWI	.		
External Idle Display			<input checked="" type="checkbox"/>

OK
Cancel

6.1.5.3 Configure PARI

Click on the **PARI** tab and enter the PARI in the System ID Field. The PARI is a user-defined system value. Enter any number from 1-292 (e.g., **4**). Click the **OK** button to continue.

The screenshot shows the 'IP-DECT Base Station' configuration window. The 'PARI' tab is selected. The 'System ID' field contains the value '4'. There are 'OK' and 'Cancel' buttons below the field.

6.1.5.4 Configure SARI

Click on the **SARI** tab. The **SARI** is an Ascom provided activation code which is needed for the system to function. Contact Ascom to obtain a **SARI**. Enter the **SARI** value (note the actual value has been hidden on the screen shown below for security reasons). Click the **OK** button to continue.

The screenshot shows the 'IP-DECT Base Station' configuration window. The 'SARI' tab is selected. The 'SARI' field contains a masked value 'XXXXXXXXXXXX'. There are 'OK' and 'Cancel' buttons below the field.

6.1.5.5 Configure Air Sync

Click on the **Air Sync** tab and select **Master** from the **Sync Mode** dropdown box. Click the **Resynchronize on command** radio button. Click the **OK** button to continue.

The screenshot shows the 'IP-DECT Base Station' configuration window. The 'Air Sync' tab is selected. The 'Sync Mode' dropdown is set to 'Master'. The 'Resynchronize on command' radio button is selected. There are 'OK' and 'Cancel' buttons at the bottom.

6.1.6. Create Users

Navigate to the **Users** and click on the **Users** tab. The **Park** value is displayed. This value can be used when programming Ascom wireless DECT handsets (optional, required only when in range of other DECT systems). Note, the **PARK** information is derived from the SARI and should be obtained from an Ascom associate (Note the actual **PARK** and **PARK 3rd pty** values have been hidden on the screen shown below for security reasons). Click the **new** link to provision a new user account.

The screenshot displays the 'IP-DECT Base Station' web interface. On the left is a navigation menu with categories: Configuration, Administration, and Device Overview. Under Configuration, options include General, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, and Services. Under Administration, options include Users and Device Overview. The main content area has tabs for 'Users' and 'Anonymous', with 'Users' selected. The 'Users' tab shows a form with the following fields: 'PARK' (with a greyed-out input), 'PARK 3rd pty' (with a greyed-out input), and 'Master Id' (with the value '0'). Below these fields are four links: 'show', 'new', 'import', and 'export'.

When the **User type** page is presented click on the **User** radio button and enter the following:

- **Long Name** Enter any descriptive name that identifies this user (i.e., **d63 5182**)
- **Display Name** Enter a display name which will be displayed on the DECT Handset screen (i.e., **5182**)
- **Name** Enter the extension assigned to this user
- **Number** Enter the extension assigned to this user
- **Password** Enter the Password (Note, the password is the **Login Code** configured in **Section 5.4**)
- **Confirm Password** Confirm Password
- **Auth. Code** Enter the **Auth. Code** (Note the Auth. Code is used only if **Subscriptions** in **Section 6.1.5.1** is set to **With System AC**)

Once all the user information has been configured, click the **OK** button. Repeat this process for each user being added to the system.

The screenshot shows a web browser window titled "Edit User - Mozilla Firefox" with the URL "10.10.40.126/GW-DECT/mod_cmd_login.xml?cmd=show&user-guid". The form contains the following fields and values:

User type	<input checked="" type="radio"/> User <input type="radio"/> User Administrator
Long Name	d63 5182
Display Name	d63 5182
Name	5182
Number	5182
Auth. Name	(SIP only)
Password	••••••••
Confirm Password	••••••••
IPEI / IPDI	110550389613
Idle Display	d63 5182
Auth. Code	
Feature Status	

Buttons at the bottom: OK, Apply, Delete, Unsubs., Cancel

6.2. Configure Ascom IP DECT handsets

Refer to the Ascom documentation in **Section 9** to obtain information on the procedures for subscribing and registering the Ascom wireless DECT handsets to the Ascom wireless IP-DECT Base Station.

7. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the IP Office and Ascom solution.

7.1. Ascom wireless DECT Handset Registration Verification

From a web browser, open a connection to the Ascom wireless IP-DECT Master Base Station (see **Section 6.1**). Navigate to the **Users** and click on the **Users** tab followed by the **show** link. A **Registration** state of “Unsubscribed” (not shown) indicates an Ascom wireless DECT handset has not registered to the Ascom wireless IP-DECT Base Station. A **Registration** state of “Subscribed” indicates that an Ascom wireless DECT Handset has connected to the Ascom wireless IP-DECT Base Station and requested the use of that particular extension. A **Registration** state that displays the IP Address of the IP Office indicates the extension has successfully registered to both the Ascom wireless IP-DECT Base Station and IP Office. The screen shot shows four DECT handsets registered to the IP Office.

IP-DECT Base Station

Configuration
Users
Anonymous

General

LAN

IP4

IP6

LDAP

DECT

VoIP

Unite

Services

Administration

Users

Device Overview

DECT Sync

Traffic

PARK

PARK

3rd

pty

Master Id

[show](#)

[new](#)

[import](#)

[export](#)

User Administrators

[Long Name](#) [Name](#)

User Administrators: 0

Users

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
d81 5184	5184	5184	+	d81 5184	002020909367		d81-Messenger	4.6.2		10.10.40.25
d81 5185	5185	5185	+	d81 5185	002020909371		d81-Messenger	4.6.2		10.10.40.25
d63 5183	5183	5183	+	d63 5183	110550389538		d63-Talker	2.2.2		10.10.40.25
d63 5182	5182	5182	+	d63 5182	110550389613		d63-Talker	2.2.2		10.10.40.25
d81 5078	5078	5078	+	d81 5078	002020772294					Subscribed
d81 5077	5077	5077	+	d81 5077	002020909369					Subscribed
d41 9923	9923	9923	+	d41 9923	085870140743					Subscribed
d62 9922	9922	9922	+	d62 9922	036470363716					Subscribed

Users: 8, Registrations: 4

8. Conclusion

A full and comprehensive set of feature and functional test cases were performed during compliance testing. The Ascom IP-DECT SIP solution is considered compliant with Avaya IP Office 11.0. All observations and issues are outlined in **Section 2.2**.

9. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from your Avaya representative.

[1] *Avaya IP Office Manager 11.0*, Release 11.0 Issue 17a August 2018

Product Documentation for Ascom Products can be obtained from Ascom or may be requested at <https://www.ascom-ws.com/AscomPartnerWeb/Templates/WebLogin.aspx> (login required).

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.